AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Amended) In a computer system with a processing device coupled to a memory device through a bus and a boot signature checker that is separate from the processing device, the computer system configured to be capable of receiving presentable content, a method of detecting tampering of the computer system, the method comprising the following:

a specific act of booting up the computer system;

a specific act of the boot signature checker monitoring a signal sequence that occurs on the computer system bus coupling the processing device and memory device during the specific act of booting up the computer system;

a specific act of the boot signature checker calculating a boot signature from the monitored signal sequence;

a specific act of comparing the calculated boot signature to an expected boot signature that represents no tampering to the computer system; and

a specific act of determining that tampering has not occurred if the calculated boot signature is the same as the expected boot signature.

2. (Canceled).

3. (Original) A method in accordance with Claim 1, further comprising the following:

a specific act of enabling presentable content to be presented if it is determined that tampering has not occurred.

4. (Original) A method in accordance with Claim 3, wherein the presentable content is encrypted presentable content, wherein the specific act of enabling presentable content to be presented comprises the following:

activating a decrypter that receives the encrypted presentable content .

5. (Original) A method in accordance with Claim 4, wherein the specific act of monitoring a signal sequence is performed by a boot signature checker circuit that is integrated with the decrypter.

6. (Original) A method in accordance with Claim 4, wherein the specific act of activating a decrypter comprises the following:

a specific act of providing the calculated boot signature directly to the decrypter, wherein the decrypter is configured to accept the expected boot signature as a key string needed to activate the decrypter.

7. (Original) A method in accordance with Claim 4, wherein the specific act of activating a decrypter comprises the following:

a specific act of providing the calculated boot signature to the decrypter; and

a specific act of the decrypter obtaining a key string needed to be activated if the calculated boot signature matched the expected boot signature.

8. (Original) A method in accordance with Claim 7, wherein the specific act of the decrypter obtain a key string comprises the following:

a specific act of the decrypter obtaining the key string from the memory device.

9. (Original) A method in accordance with Claim 1, further comprising the following:

a specific act of determining that tampering has occurred if the calculated boot signature is different than the expected boot signature.

10. (Original) A method in accordance with Claim 9, further comprising the following:

a specific act of blocking the presentation of the presentable content if it is determined that tampering has occurred.

11. (Previously Amended) A method in accordance with Claim 10, wherein the specific act of blocking the presentation of the presentable content comprises the following:

a specific act of deactivating a decrypter that receives the presentable content.

12. (Original) A method in accordance with Claim 10, wherein the specific act of blocking the presentation of the presentable content comprises the following:

a specific act of disabling a demodulator such that the demodulator does not demodulate the presentable content.

13. (Original) A method in accordance with Claim 10, wherein the specific act of blocking the presentation of the presentable content comprises the following:

a specific act of disabling a tuner such that the tuner does not tune to the presentable content.

14. (Original) A method in accordance with Claim 10, wherein the specific act of blocking the presentation of the presentable content comprises the following:

disabling a central processing unit clock.

15. (Original) A method in accordance with Claim 10, wherein the specific act of blocking the presentation of the presentable content comprises the following:

disabling a demultiplexor such that audio, video or other data cannot be extracted from the presentable content.

16. (Original) A method in accordance with Claim 10, wherein the specific act of blocking the presentation of the presentable content comprises the following:

disabling a network interface device used by the computer system to interface with a network.

17. (Original) A method in accordance with Claim 1, wherein the specific act of calculating a boot signature that is a function of the signal sequence comprises the following:

calculating the boot signature by applying a polynomial expression to the signal sequence.

18. (Previously Amended) In a computer system with a processing device coupled to a memory device through a bus and a boot signature checker that is separate from the processing device, the computer system configured to be capable of receiving presentable, a method of detecting tampering of the computer system, the method comprising the following:

a specific act of booting up the computer system;

a step for the boot signature checker producing a boot signature that is a function of a signal sequence experienced on the computer system bus between the processing device and the memory device during the specific act of booting; and

a step for determining whether the calculated boot signature is indicative of the computer system being tampered with.

19. (Canceled).

20. (Original) A method in accordance with Claim 18, wherein the step for calculating a boot signature comprises the following:

a specific act of monitoring the signal sequence during the specific act of booting up the computer system; and

a specific act of calculating the boot signature as a function of the signal sequence monitored during the specific act of monitoring.

21. (Previously Amended) A method in accordance with Claim 20, wherein the specific act of monitoring the signal sequence comprising the following:

a specific act of a boot signature checker monitoring the bus to determine the signal sequence that occurs on the bus during the specific act of booting up the computer system.

22. (Original) A method in accordance with Claim 18, further comprising:

a step for acting on the determination of whether the calculated boot signature is indicative of the computer system being tampered with.

23. (Original) A method in accordance with Claim 22, wherein the step for acting on the determination comprises the following:

a specific act of activating a decrypter so as to enable the decrypter to decrypt the presentable content.

24. (Original) A method in accordance with Claim 23, wherein the specific act of activating a decrypter comprises the following:

a specific act of providing the calculated boot signature directly to the decrypter, wherein the decrypter is configured to accept an expected boot signature as a key string needed to activate the decrypter.

25. (Previously Amended) A computer system capable of receiving presentable content, wherein the computer system comprises:

a processing device;

a memory device;

a local bus coupled to the processing device and the memory device;

a decrypter configured to decrypt encrypted content when activated; and

a boot signature checker, separate from the processing device, that is coupled to the local bus so as to be able to read a signal sequence asserted on the local bus during booting of the computer system,

wherein the boot signature checker is configured to calculate a boot signature from the signal sequence asserted on the local bus coupling the processing device and the memory device.

26. (Original) A computer system in accordance with Claim 25, wherein the boot signature checker is directly coupled to the bus.

27. (Original) A computer system in accordance with Claim 25, wherein the boot signature checker is coupled to the decrypter so as to provide the boot signature to the decrypter.

28. (Original) A computer system in accordance with Claim 25, wherein the boot signature checker and the decrypter are integrated within a single physical device.

29. (Previously Amended) A computer system capable of decrypting encrypted content, wherein the computer system comprises:

a processing device;

a memory device;

a bus coupled to the processing device and the memory device;

a decrypter configured to decrypt encrypted content when activated; and

means for calculating a boot signature, separate from the processing device, that is a function of the signal sequence experienced on the computer system bus between the processing device and the memory device during booting up of the computer system.

30. (Previously Amended) A computer system in accordance with Claim 29, wherein the means for calculating a boot signature comprises the following:

a processing device;

a memory device;

a bus coupled to the processing device and to the memory device of the means for calculating a boot signature; and

a boot signature checker that is coupled to the computer system bus so as to be able to monitor the bus for signal sequences.

31. (Original) A computer system in accordance with Claim 30, further comprising the following:

a decrypter; and

a dedicated connection connecting the boot signature checker with the decrypter.

32. (Previously Presented) A computer system in accordance with Claim 30, wherein the boot signature checker, the dedicated connection, and the decrypter are integrated within a single physical device.